

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
APO AE 09128

22 SEP 1994

DIRECTIVE
NUMBER 55-38

OPERATIONS

Command and Control Warfare (C2W)

1. Summary. This directive establishes policy, assigns responsibilities, and prescribes procedures for the employment of Command and Control Warfare (C2W) operations within the USCINCEUR unified command.

2. Applicability. This directive applies to HQ USEUCOM, service components, assigned and attached forces, and Joint Task Forces.

3. Suggested Improvements. Recommendations for changes and improvements to this directive should be submitted to the Operations Directorate/Operations Plans Division, office symbol ECJ35.

4. References. See Appendix A.

5. Explanation of Terms.

a. Command and Control Warfare. The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control (C2) capabilities, while protecting friendly C2 capabilities against such actions. Also called C2W.

b. C2W is both offensive and defensive:

(1) Counter-C2. To prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the

adversary C2 system.

(2) C2-Protection. To maintain effective C2 of own forces or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.

c. See Appendix B for additional terminology.

6. Responsibilities.

a. Director of Intelligence, ECJ2, with functional support from the Joint Analysis Center (JAC), Molesworth UK, will:

(1) Provide a point of contact (POC) to be responsible for coordinating C2W matters and participate in C2W working groups.

(2) Address C2W into plans, operations, and publications.

(3) Correlate Joint Operation Planning and Execution System (JOPES) Appendix 6 (support to EW and C2W) and Appendix 8 (support to OPSEC, PSYOP, and Deception) to Annex B (Intelligence) with Appendix 10 to Annex C in accordance with (IAW) CJCS MOP 30, para 16b(3)(b) guidance.

(4) Provide intelligence support to C2W as specified in Appendix C.

b. Director of Operations, ECJ3, will:

(1) Maintain primary responsibility for all C2W matters within USEUCOM.

This Directive supersedes ED 55-38, 5 Feb 86.

22 SEP 1994

(2) Administer C2W working groups.

(3) Prepare C2W input into USCINCEUR plans, operations, and exercises.

(4) Prepare JOPES Appendix 10 to Annex C (Operations) as the C2W appendix IAW CJCS MOP 30, para 16b(3)(a) guidance. Correlate Appendix 3 (EW), Appendix 4 (PSYOP), and Appendix 7 (Deception) to Annex C; and Annex L (OPSEC) in preparation of Appendix 10.

(5) Identify requirements for Special Technical Operations (STO) support to C2W operations.

(6) Secure C2W training opportunities and incorporate C2W into exercises IAW Appendix D.

(7) Prepare C2W inputs to CINC's Preparedness and Assessment Report (CSPAR), Joint Universal Lessons Learned (JULLS), and Joint Mission Essential Task List (JMETL) as required.

c. Director of Command, Control and Communications Systems, ECJ6, will:

(1) Provide a POC to be responsible for coordinating C2W matters and participate in C2W working groups.

(2) Address C2W into plans, operations, and publications.

(3) Correlate JOPES Appendix 2 (C3 Protection) and Appendix 6 (Frequency Management) to Annex K (C3 Systems) with Appendix 10 to Annex C IAW CJCS MOP 30, para 16b(3)(b) guidance.

d. HQ JTF will:

(1) Establish JTF/C2W Officer and staff representation.

(2) Execute Joint C2W procedures IAW paragraph 9 of this directive.

(3) Prepare OPLAN Appendix 10 to Annex C as discussed above in

paragraph 7b(4).

e. Service component commanders will:

(1) Designate an office of primary responsibility and POC to be responsible for coordinating C2W matters and participate in C2W working groups called by HQ USEUCOM.

(2) Promote joint training of principal C2W personnel via formal classes offered in Appendix D.

(3) Support Joint C2W operational taskings and exercises.

f. Chief National Security Agency/Central Security Service Europe (NCEUR) will:

(1) Provide a POC to be responsible for coordinating C2W matters and participate in C2W working groups.

(2) Provide SIGINT and Information Security (INFOSEC) support as they pertain to C2W.

7. Policy.

a. C2W shall be integrated into theater strategy, concepts, plans, operations, exercises, and training in order to maximize U.S. and allied military effectiveness against current and projected adversaries.

b. C2W strategies will be developed so they are compatible and supportive in joint and allied operations to the maximum extent practicable. U.S. C2W planners must constantly consider the integration of U.S. forces into NATO or coalition operations.

c. Personnel will be trained and C2W exercised to the maximum extent practical in such a manner to permit measurement of C2W objective achievement (see Appendix D).

d. Joint C2W strategy will be supported by commanders of USNAVEUR, MARFOREUR, USAREUR, USAFE, and external forces assigned to USEUCOM. Close coordination is essential for

complementary actions and the avoidance of fratricide.

8. Procedures.

a. C2W Concept.

(1) Modern military forces are highly dependent upon timely and accurate information conveyed through a resilient C2 system for effective application of combat power. C2 functions are performed through an arrangement of intelligence, communications, facilities, personnel, procedures, and leadership decisions derived from information and perceptions. Additionally, leadership control of forces is dependent on morale and loyalty. Each C2 element is vulnerable, in varying degrees, to OPSEC, military deception, PSYOP, EW, and destruction. Actions that degrade one or more of these elements degrade the C2 system as a whole and introduce elements of doubt into the command structure. Thus, opportunities exist for U.S./Allied employment of counter-C2 to exploit adversary weakness.

(2) Likewise, adversary forces have the capability to plan and execute counter-C2 attacks against U.S./Allied forces. Additionally, friendly actions generates interference and fratricide to own forces. The advent of modern C2 systems contributes to our ability to maintain effective C2 but simultaneously becomes our own vulnerability. Military commanders must undertake C2-protection to retain their capability to obtain valid information of the battlefield and direct forces accordingly.

(3) It is neither possible nor desirable to counter every hostile C2 activity because of the sheer numbers involved and the exceptional value of some activities as sources of intelligence. However, strategy that can integrate all five actions (OPSEC, PSYOP, deception, EW, destruction) offers friendly commanders the opportunity to corrupt adversary command and control of their forces.

(4) Intelligence support is absolutely critical to C2W. Hostile C2 nodes must be identified, located, and prioritized for counter-C2 planning. National intelligence agencies can aid in identifying the phases when these C2 nodes become critical. Knowledge of hostile C2W capabilities is necessary for planning C2-protection.

(5) Frequency management is essential to the success of C2W. All countries manage the spectrum within their national boundaries with final authority on usage being an internationally recognized sovereign right. Efficient management of the finite spectrum, which is shared by all civil and military users, both friendly and enemy, is paramount to successful communications, intelligence, and operational missions in support of C2W.

b. C2W Process.

(1) C2W is a supporting strategy whose concept is developed from the Joint Force Commander's (JFC) mission and concepts. C2W as a means to itself is meaningless.

(2) C2W support to joint military operations will normally be planned by a JTF/C2W staff element and executed by the components. As a minimum, a dedicated JTF/C2W officer is essential to translate the JFC's campaign level intentions into executable C2W support plans. (NOTE: A JTF/C2W officer line number will be included in the next revision to USEUCOM JTF HQ SOP publication, ED 55-11, Appendix A, Ref I). USEUCOM C2W Officer will provide to the JTF a C2W Reference Book in accordance with para 9g of this directive.

(3) Remaining C2W staff element should be tailored to the JTF's mission, which may consist of one or multiple operations other than war or combat operations. Level of C2W effort will determine the need for either a standing C2W staff (for major warfighting operations) or by C2W committee (for ad hoc requirements).

22 SEP 1994

(4) A generic C2W staff consist of the following representatives:

(a) C2W officer (dedicated position)--maximum access to capture JTF mission, tasks, commanders intent, policy, ROE. Prepare Appendix 10 to Annex C.

(b) OPSEC officer--interface to Joint OPSEC Program. Coordinate Annex L.

(c) PSYOP planner--interface with Joint PSYOP Task Force (JPOTF) or equivalent PSYOP organization. Coordinate Appendix 4 to Annex C.

(d) Deception planner--interface to Deception Staff Element (DSE). Coordinate Appendix 7 to Annex C.

(e) Electronic warfare officer--interface with Joint Commanders Electronic Warfare Staff (JCEWS). Coordinate Appendix 3 to Annex C.

(f) Targeting officer--interface to Joint Targeting Coordination Board (JTCB) for target nominations.

(g) Special Technical Operations (STO) representative--support as required.

(h) J2 representative--interface to intelligence collection management and JAC. Coordinate Appendix 6 and Appendix 8 to Annex B.

(i) J6 representative--interface to Joint Frequency Management Office (JFMO) and identify friendly critical nodes requiring C2-Protection. Coordinate Appendix 2 and Appendix 6 to Annex K.

(j) Joint Force Air Component Commander (JFACC) representative--interface to mission tasking.

(k) Component liaison--interface to service C2W capabilities.

(5) C2W Augmentation. Military drawdown has reduced in-theater experts and planners. CONUS reorganization fills theater shortages by providing to warfighting commanders deployable support teams

and C2W assets, some which are no cost to the commander. Liaison is essential for smooth transition to crisis. See Appendix E for C2W augmentation.

c. C2W Planning Guidance.

(1) A five step planning process is utilized to ensure C2W supports the JTF mission. Comprehensive details are found in Joint Pub 3-13, chapter VI (Appendix A, Ref H), and should be a document possessed by the JTF/C2W Officer. The JTF/C2W Officer's role is not to manage the five tools, but to coordinate and guide the planning process through a C2W viewpoint.

(a) Step One. Analyze the Joint Force Commanders's (JFC) mission and concept of operations to derive a supporting concept of C2W operations for both Counter-C2 and C2-Protect. Each campaign phase is analyzed separately. Product: Concept of C2W support.

(b) Step Two. Perform C2W analysis. For Counter-C2, identify adversary C2 systems that allow the adversary to react to friendly initiatives. For C2-Protect, identify adversary counter-C2 systems that threaten friendly C2 architecture. Conduct nodal analysis for both to determine nodes that are both critical and vulnerable. See Appendix B for node definition. Product: List of critical/vulnerable nodes for Counter-C2 and C2-Protect consideration.

(c) Step Three. Prioritize the critical/vulnerable nodes identified in Step Two into one priority list. Product: Adversary C2 node priority list for C2W targeting.

(d) Step Four. Identify the desired C2W effect (deny information, influence, degrade, or destroy) on a particular adversary node and then determine which of the five C2W tools will best achieve this effect for resource assignments. Synergistic effect should be kept in mind. Product: J3 approved C2W plan. End result is component taskings via

OPLAN (Appendix 10 to Annex C) and cyclic tasking documents such as the Air Tasking Order (ATO) or frag order.

(e) Step Five. C2W feedback. This requires C2W planners and J2 staff to agree upon an effectiveness measurement criteria. Product: Feedback loop to adjust C2W plans.

d. C2W Warfighting Tools Cross-Reference.

(1) Critical nodes identified for C2W targeting must be vulnerable (susceptible, accessible, feasible) by one or more of the C2W tools.

(2) Following guide provides a brief summary on matching tools for desired effects.

EFFECT PRIMARY TOOL SUPPORT TOOLS

Deny Info	OPSEC	PSYOP, EP Deception, Destruction
Influence	Deception	OPSEC, PSYOP, EA, EP, Destruction
Degrade	Destruction	EA, PSYOP, OPSEC, Deception

Destruction Destruction EA

(3) C2W tool selection criteria are dependent on target knowledge and ROE restrictions during phases of a conflict buildup.

(a) OPSEC is the C2W tool to deny adversary knowledge of the friendly plan, and supports the deception plan. Though OPSEC has many administrative procedures that protects routine friendly information, the C2W officer's focus is protection of critical phases of the campaign plan. OPSEC should be applied over the continuum of conflict.

(b) PSYOP conveys selected truthful information to targeted audiences with intentions to influence emotions, motives,

objective reasoning, and ultimately behavior. PSYOP can attempt to separate subordinates from their leadership, spread distrust amongst political/military leadership, or to build consensus between rival groups/persons to defy enemy authority. PSYOP can target individuals or groups. PSYOP programs can support all phases of the operational continuum and in operations other than war. A thorough understanding of the targeted population's cultural beliefs and ideology is critical.

(c) Deception requires an understanding of adversary leadership biases and presentation of a believable story to reinforce these biases. The deception planner should be knowledgeable of the OPSEC plan since both tools are interrelated (OPSEC hides the real, deception shows the fake).

(d) Electronic warfare requires the targeted equipment be active and its parametrics known. Timing is critical--the first few minutes of jamming has the biggest payoff before the affected operator has time to find a work around countermeasure. Electronic deception requires knowledge of adversary ES and SIGINT capabilities.

(e) Destruction requires precise target location, accessibility by available weapon delivery means, and have acceptable risk factor. Destruction effects are relatively short term as the adversary recovers and rebuilds alternate C2 means. Destruction requires National Command Authority approval, and normally becomes the last tool that can be executed over the operational continuum.

e. C2 Protection.

(1) C2-Protect is partly performed by attacking adversary counter-C2 capabilities (paragraph 9c) and by default friendly C2 vulnerabilities are reduced. However, coordination and tasking requirements exist to cover other aspects of C2-Protect. Friendly

22 SEP 1994

force C2 vulnerabilities must be identified, evaluated, prioritized, and assigned a level of protection required.

(2) Additional C2-Protect requirements.

(a) Reduce friendly C2 vulnerabilities by assigning C2-protection (theater missile defense, combat air patrol, force protection, etc) to critical nodes.

(b) Minimize friendly electronic interference and fratricide through frequency management. The Joint Restricted Frequency List (JRFL) is

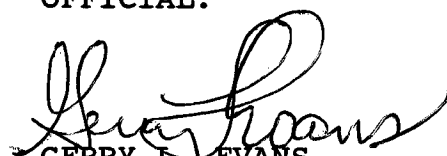
the established joint tool, published by the J6/JFMO, closely coordinated between J2/J3/J6 (normally via the forum of the Joint Commander's Electronic Warfare Staff--JCEWS), and approved by the J3.

f. Authority. Authority for C2W actions and means will be in accordance with CJCS MOP 30, para 15.

g. C2W Reference Book. HQ USEUCOM C2W proponent identified in para 3 of this publication will build and maintain a C2W Reference Book tailored to assist the JTF/C2W Officer. Asterisk items in Appendix A, POC list, and sample Appendix 10 to Annex C will be included.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:


GERRY L. EVANS
MAJ, USA
Acting Adjutant General

RICHARD F. KELLER
Lieutenant General, USA
Chief of Staff

Appendixes:

- A. References
- B. Explanation of Terms
- C. Intelligence Support to C2W
- D. Training and Exercises
- E. C2W Augmentation

DISTRIBUTION:

ECJ1/ECJ1-A	2	ECPA	1
ECJ2/ECJ2-P	2	ECSO	1
ECJ3/ECJ35	10	NCEUR	1
ECJ4	1	HQ USAFE	4
ECJ5	1	NAVEUR/N9	4
ECJ6/ECJ6-DF	2	USAREUR/AEAGC-P-PC	4
ECLA	1	MARFOREUR/G5	4

Appendix A

REFERENCES

- a.* CJCS Memorandum of Policy No. 30, 8 March 1993, Command and Control Warfare (U) (UNCLASSIFIED).
- b. CJCS Memorandum of Policy No. 6, 3 March 1993, Electronic Warfare (U) (SECRET).
- c. CJCS Memorandum of Policy No. 116, 24 March 1987, Military Deception (U) (SECRET).
- d. CJCS INST 3213.01, 28 May 1993, Joint Operations Security (U) (UNCLASSIFIED).
- e. CJCS INST 3220.01, DRAFT, Electromagnetic Spectrum Use in Joint Military Operations (U) (UNCLASSIFIED).
- f.* CJCS INST 5118.01, Charter for the Joint Command and Control Warfare Center (U) (UNCLASSIFIED).
- g. NATO Military Committee Document MC 290, NATO Counter C3 Policy (U) (UNCLASSIFIED), in rewrite as MC 290/1-NATO Command and Control Warfare (U) (UNCLASSIFIED).
- h.* Joint Pub 3-13, DRAFT, Joint Command and Control Warfare Operations (U) (SECRET).
- i. USEUCOM Directive 55-11, 29 May 92, Joint Task Force Headquarters Organization and Standing Operating Procedures (U) (UNCLASSIFIED).
- j. USEUCOM Directive 100-6, 01 June 1984, Radio Frequency Spectrum Management (U) (UNCLASSIFIED).
- k. EUCOM Tactics, Techniques, and Procedures (ETTP), ECJ2 Publication, 20 August 1993 (U) (SECRET/NOFORN/WNINTEL)

* Identifies references for immediate need by JTF/C2W Officer, which will be made available by the USEUCOM provided C2W Reference Book (see para 9g to this directive)

Appendix B

EXPLANATION OF TERMS

B-1. The following terminology applies; * designates definitions for purposes of this directive only.

B-2. Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures that are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

B-3. Critical Node. * An element, position, or communications entity whose disruption or destruction immediately degrades the ability of a force to command, control or effectively conduct combat operations.

B-4. Electronic Warfare (EW). Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support. (Proposed by CJCS MOP 6 for inclusion in Joint Pub 1-02 as change to current definition).

a. Electronic attack. That division of electronic warfare involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, RF weapons, particle beams).

b. Electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP.

c. Electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated

Appendix B

EXPLANATION OF TERMS (cont)

electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical action such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be use to produce signals intelligence (SIGINT), both communications intelligence (COMINT) and electronic intelligence (ELINT).

B-5. Joint Restricted Frequency List. A list of protected, guarded, or taboo frequencies promulgated by a CINC or JTF commander in order to protect critical friendly frequencies or nets from friendly EW. Also called JRFL.

B-6. Military Deception. Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. There are three categories of military deception:

a. Strategic Military Deception. Military deception planned and executed to result in foreign national policies and actions which support the originator's national objectives, policies, and strategic military plans.

b. Tactical Military Deception. Military deception planned and executed by and in support of operational commanders against the pertinent threat, to result in opposing operational actions favorable to the originator's plans and operations.

c. Department/Service Military Deception. Military deception planned and executed by Military Services about military systems, doctrine, tactics, techniques, personnel or service operations, or other activities to result in foreign actions which increase or maintain the originator's capabilities relative to adversaries.

B-7. Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

Appendix B

EXPLANATION OF TERMS (cont)

b. Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

B-8. Physical Destruction. Hard kill weapons effects.

B-9. Psychological Operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

B-10. Vulnerable Node.* A node having an exploitable and viable weakness against available resources. It must be susceptible to degradation, be accessible, and feasible in assuming risks involved with attempts to degrade the node.

Appendix C

INTELLIGENCE SUPPORT TO C2W

C-1. Purpose. To establish guidelines for providing intelligence support to C2W.

C-2. General. Integrated intelligence and counterintelligence support is critical to C2W. Emphasis should be placed on critical node analysis and target development. This nodal analysis and the commander's intent will be the basis upon which C2W plans and tactics are developed.

C-3. Support Guidelines. Intelligence support generally includes:

a. Developing and maintaining data bases of sufficient detail to create a C2 network model in geographic areas of potential conflict.

b. Identify critical C2 nodes, links, sensors, and layers of C2 networks utilized by potentially hostile nations. Include general target types, critical times of vulnerability associated with each type, and sufficiently detailed information on key targets for weaponeering. Particularly required is an understanding of hostile C2, communications, sensor systems, peacetime-wartime-reserve operating modes, redundancy, organizational structure, procedures, and deployment.

c. Identify the key political and military leaders in potentially hostile nations. Address both formal and informal power structures. Provide biographical data and, when available, psychological assessments to support the PSYOP element of C2W.

d. Estimating hostile counter-C2 capabilities to determine the vulnerability of U.S. and NATO C2 capabilities.

e. Providing timely and reliable indications and warning information to operational commanders.

f. Supporting battle damage assessments associated with C2W operations.

C-4. Exchange of military information within NATO is required to enhance both U.S. and allied C2W planning and execution. USEUCOM/J2 publication "EUCOM Tactics, Techniques and Procedures" (Appendix A, reference k) describes intelligence organization and information flow support.

Appendix D

TRAINING AND EXERCISES

D-1. Purpose. To provide guidance and procedures for incorporating C2W into training and exercises within USEUCOM.

D-2. Guidance.

a. Key personnel associated with C2W should attend formal joint C2W courses.

b. C2W should be an objective in joint and combined exercises when the opportunity avails itself. C2W staffs should be exercised and equipment tested when allowed.

c. Exercise conditions should be representative of theater C2W wartime environment or anticipated scenarios.

d. Tactics and techniques should be validated and equipment performance verified during exercise activities. Document deficiencies.

e. Exercises will be protected with appropriate security measures, OPSEC, and avoid electromagnetic interference with allied and host country systems.

D-3. Procedures.

a. Education. The HQ USEUCOM C2W Officer is the command focal point for disseminating course information and coordinating billet request for course attendance. Units desiring student billets are requested to contact HQ USEUCOM/ECJ35. The following courses are directly managed through ECJ35.

(1) Joint C2W Staff Officers Course (JC2WSOC), two weeks, Norfolk VA.

(2) Joint EW Staff Officers Course (JEWSOC), two weeks, Norfolk VA.

(3) NATO Counter C3 Course (I-19 series), one week, Oberammergau GE.

(4) NATO EW Courses (I-41, I-42, I-43 series), one or two weeks, Oberammergau GE.

Coordination can be made for other related courses.

Appendix D

TRAINING AND EXERCISES (Cont)

- (5) Joint Senior Leaders C2W Course (JSLCC)
- (6) Joint Military Planners Course (JMPC)
- (7) Joint PSYOP Staff Planners Course (JPSPC)

b. Training and Exercises.

(1) Establish realistic C2W objectives. Examples are Appendix 10 to Annex C development for a HQ JTF standup exercise, and the proper use of a JRFL for C2-protect during an offensive air campaign.

(2) The commander is responsible for overall planning to consider the following:

(a) Avoid misleading other nations to conclude that hostilities are intended.

(b) Coordinate with cognizant frequency managers to comply with peacetime restrictions and obtain host country authorization. Frequency clearances requires several months lead time.

c. Report C2W lessons learned in exercise reports and document them in the joint universal lessons learned (JULLs) with HQ USEUCOM/ECJ37 (Exercise Division). Innovative techniques and methods developed that have real-world application should be highlighted.

d. Input Joint Mission Essential Task List (JMETL) requirements with ECJ37.

Appendix E

C2W AUGMENTATION

E-1. Purpose. To identify other C2W assets available for supporting European Theater operations.

E-2. Situation. Military drawdown has reduced staff expertise and manpower for thorough C2W planning. To fill this void, CONUS military reorganization provides C2W support to the warfighting commander. Listed below are CONUS resources (subject to change as the C2W concept matures and agencies realign appropriately).

E-3. C2W Assets.

(1) Joint Electronic Warfare Center (JEWEC), San Antonio TX, provides deployable C2W and EW support teams to augment existing staffs with specialists. Teams deploy with unit owned equipment to maintain electronic connectivity with their center for responsive analytical support. Major contributions are C2W and EW planning staffs, Country C2W Analysis and Decision Aids, EW Predictive Analysis, and engineering support. JEWEC deployments and services are cost free to USCINCEUR. JEWEC will be renamed the Joint C2W Center (JC2WC), date to be determined, and is described in Appendix A, Ref F.

Message address: JEWEC SAN ANTONIO TX//DV/OP//

Phone:

DSN 969-2192/2151 (24-hrs Operations Support Center)

DSN 969-4735 (USEUCOM Team Chief)

Commercial prefix 210-977-xxxx.

(2) Electromagnetic Compatibility Analysis Center (ECAC), Annapolis MD, provides frequency management support, spectrum data bases, and can deploy specialist as required. Major contributions are Joint Frequency Management Office (JFMO) support, Joint Restricted Frequency List (JRFL) support, Joint Spectrum Interference Resolution program administration (formally called MIJI), and production of products useful for PSYOP broadcast/transmission planning. ECAC will eventually be absorbed into a new agency, the Joint Spectrum Center. Deployments and services will at a later date become cost free to the warfighting commander. Coordinate ECAC support with J6.

Message address: ECAC ANNAPOLIS MD//CJ//

Phone: DSN 281-4956, Comm 410-267-4956.

(3) Defense Intelligence Agency (DIA) can support C2W data bases, decision aids, and targeting support. DIA C2W office POC is DIW-IC.

Message Address: DIA WASHINGTON DC//DIW-IC//

Phone: DSN 243-3554/3367, Comm 312-243-3367.

22 SEP 1994

Appendix E

C2W AUGMENTATION

(4) National Security Agency (NSA), provides support to the warfighter. G71 is the initial POC for requests.

Message Address: DIRNSA FT GEORGE G. MEADE MD//G71//

Phone: DSN 644-6404/6405

(5) USEUCOM Special Technical Operations (STO). The C2W Officer must ensure the STO representative is read into all phases of C2W activities. STO representative will then provide support as required. Coordinate for STO support through HQ USEUCOM/ECJ35, DSN 430-4294/5096, Comm 49-711-680-4294.

(6) The 4th Psychological Operations Group (Airborne) (4th POG [A]) can support C2W by providing staff augmentation, liaison elements, PSYOP planning, and PSYOP execution. All active component PSYOP assets are within the 4th POG (A). Additionally, the 4th POG (A) exercises training authority over all U.S. Army Reserve component PSYOP units. Coordinate for PSYOP support through HQ USEUCOM/ECJ35, DSN 430-4284/8314, Comm 49-711-680-4284.

(7) U.S. SPACE COMMAND (USSPACECOM). USSPACECOM provides unique capabilities to supplement counter-C2 and C2-protect aspects of C2W. Major contributions are communications, navigation, reconnaissance, and space control. Dialogue with USSPACECOM geographic POC is required to determine the full extent of capabilities they offer. Support teams are cost free to USCINCEUR.

Message address: USCINCSpace PETERSON AFB CO//SPJ33S//

Phone: DSN 692-5943, Comm 719-554-5943.